



PCT

特許協力条約に基づいて公開された国際出願

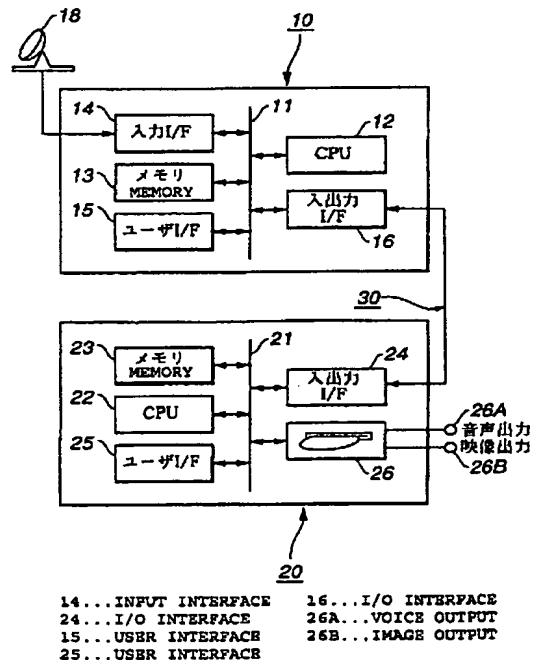
(51) 国際特許分類 H04L 9/08, 9/32, 12/40, H04N 7/167		A1	(11) 国際公開番号 WO00/62476
		(43) 国際公開日 2000年10月19日(19.10.00)	
(21) 国際出願番号 PCT/JP00/02354		(81) 指定国 JP, US	
(22) 国際出願日 2000年4月11日(11.04.00)		添付公開書類 国際調査報告書	
(30) 優先権データ 特願平11/105965 1999年4月13日(13.04.99) JP			
<p>(71) 出願人 (米国を除くすべての指定国について) ソニー株式会社(SONY CORPORATION)[JP/JP] 〒141-0001 東京都品川区北品川6丁目7番35号 Tokyo, (JP)</p> <p>(72) 発明者: および</p> <p>(75) 発明者/出願人 (米国についてのみ) 浅野智之(ASANO, Tomoyuki)[JP/JP] 大澤義知(OSAWA, Yoshitomo)[JP/JP] 小室輝芳(KOMURO, Teruyoshi)[JP/JP] 石黒隆二(ISHIGURO, Ryuji)[JP/JP] 〒141-0001 東京都品川区北品川6丁目7番35号 ソニー株式会社内 Tokyo, (JP)</p> <p>(74) 代理人 小池 晃, 外(KOIKE, Akira et al.) 〒105-0001 東京都港区虎ノ門二丁目6番4号 第11森ビル Tokyo, (JP)</p>			

(54) Title: DATA TRANSMISSION SYSTEM

(54) 発明の名称 データ伝送システム

(57) Abstract

An encryption key is produced by 1st information owned secretly in common with a data receiver (20), 2nd information introduced from duplication control information of transmission data and 3rd information which is time modulation information owned in common with the data receiver. Data are encrypted by a CPU (12) using the encryption key. Transmission data which are obtained by adding the duplication control information data and the time modulation information to the encrypted data are transmitted to the data receiver (20) from a data transmitter (10).



(57)要約

データ受信装置 20 との間で秘密に共有されている第 1 の情報と、送信データの複製制御情報から導かれる第 2 の情報と、上記データ受信装置との間で共有する時変情報である第 3 の情報によって暗号鍵を生成し、この暗号鍵を用いてデータを CPU 12 により暗号化し、暗号化したデータに時変情報を上記複製制御情報及び時変情報を付加した送信データをデータ送信装置 10 からデータ受信装置 20 に送信する。

PCTに基づいて公開される国際出願のパンフレット第一頁に掲載されたPCT加盟国を同定するために使用されるコード(参考情報)

AE	アラブ首長国連邦	DM	ドミニカ	KZ	カザフスタン	RU	ロシア
AG	アンティグア・バーブーダ	DZ	アルジェリア	LC	セントルシア	SD	スーダン
AL	アルバニア	EE	エストニア	LI	リヒテンシュタイン	SE	スウェーデン
AM	アルメニア	ES	スペイン	LK	スリランカ	SG	シンガポール
AT	オーストリア	FI	フィンランド	LR	リベリア	SI	スロヴェニア
AU	オーストラリア	FR	フランス	LS	レソト	SK	スロヴァキア
AZ	アゼルバイジャン	GA	ガボン	LT	リトアニア	SL	シエラ・レオネ
BA	ボスニア・ヘルツェゴビナ	GB	英国	LV	ルクセンブルグ	SN	セネガル
BB	バルバドス	GD	グレナダ	MA	モロッコ	SZ	スワジランド
BE	ベルギー	GE	グルジア	MC	モナコ	TD	チャード
BG	ブルガリア	GH	ガーナ	MD	モルドヴァ	TG	トーゴ
BJ	ベナン	GM	ガンビア	MG	マダガスカル	TJ	タジキスタン
BR	ブラジル	GN	ギニア	MK	マケドニア	TM	トルクメニスタン
BS	バハマ	GR	ギリシャ		旧ユーゴスラヴィア	TR	トルコ
BY	ベラルーシ	GW	ギニア・ビサウ		共和国	TT	トリニダード・トバゴ
CA	カナダ	HU	クワチア	ML	マリ	TZ	タンザニア
CC	中東アフリカ	ID	インドネシア	MN	モンゴル	UG	ウガンダ
CG	コンゴ	IE	アイルランド	MR	モーリタニア	US	米国
CH	スイス	IL	イスラエル	MW	マラウイ	UZ	ウズベキスタン
CI	コートジボワール	IN	インド	MX	メキシコ	VN	ヴェトナム
CM	カメルーン	IT	イタリア	MZ	モザンビーク	YU	ユーゴスラヴィア
CN	中国			NE	ニジェール	ZA	南アフリカ共和国
CR	コスタ・リカ			NL	オランダ	ZW	ジンバブエ
CU	キューバ			NO	ノルウェー		
CY	キプロス			NZ	ニュージーランド		
CZ	チェコ			PL	ポーランド		
DE	ドイツ			PT	ポルトガル		
DK	デンマーク			RO	ルーマニア		
		KR	韓国				

## 明細書

### データ伝送システム

### 技術分野

本発明は、データ送信装置からデータ受信装置にデータを伝送するデータ伝送システム、データ伝送方法、データ送信装置、データ送信方法、データ受信装置及びデータ受信方法に関する。

### 背景技術

近年、例えば家庭内において、複数のＡＶ機器をデジタルインターフェースを介して接続し、音楽情報や映像情報などのデジタルデータを伝送したり記録したりするようにしたシステムが普及しつつある。例えば、デジタルバスであるＩＥＥＥ(The International of Electrical and Electronics Engineers, Inc.) 1394ハイ・パフォーマンス・シリアル・バス規格(以下、単にＩＥＥＥ1394シリアルバスという)のインターフェースを持つビデオカメラやDigital Versatile Disk(DVD)(商標)プレーヤなどのＡＶ機器が開発されている。

ところで、通常、映画データ等は著作権のある情報であり、不正

なユーザによるコピー等を防ぐ必要がある。

不正なユーザによるコピー等を防ぐために、例えば、ミニディスク(MD) (商標) システムにおいては、SCMS (Serial Copy Management System) と呼ばれる方法が用いられている。これは、デジタルインタフェースによって、音楽データとともに伝送される情報のことである。この情報は、音楽データが、copy free、copy once allowed、又はcopy prohibited のうちのいずれのデータであるのかを表す。ミニディスクレコーダは、デジタルインタフェースから音楽データを受信した場合、SCMSを検出し、これが、copy prohibited であれば、音楽データをミニディスクに記録せず、copy once allowed であれば、SCMS情報をcopy prohibited に変更すると共に、受信した音楽データとともに記録し、copy freeであれば、SCMS情報はそのまま受信した音楽データとともに記録する。

このようにして、ミニディスクシステムにおいては、SCMSを用いて、著作権を有するデータが不正にコピーされるのを防いでいる。

また、デジタルインタフェースを介して音楽情報や映像情報などのデジタルデータを伝送したり記録したりするようにしたデータ伝送システムでは、伝送路上のデータパケットのパケットヘッダに、複製制御情報を格納して送る方式が考えられている。

この複製制御情報は、例えば次のように

00 : コピー制限なし

10 : 1回のみコピー可

01 : これ以上のコピー禁止

11 : もともとコピー禁止 2ビットで定義されている。

データパケットを受信した記録機器は、データを記録する際に、複製制御情報を検査し、複製制御情報が「0 1」又は「1 1」すなわちコピー禁止を表していれば受信したデータの記録を行わない。また、複製制御情報が「1 0」すなわち1回のみコピー可を表していれば、複製制御情報を「0 1」すなわちこれ以上のコピー禁止に変更してから受信データを記録メディアに記録する。

このようにして、もとのデータから生じるコピーの世代を制限するようにしている。

さらに、このコピー世代の制限方式に強制力を持たせるために、データを暗号化して伝送し、コピー世代制限方式を遵守する機器のみを製造するという契約を交わしたメーカーにのみ、暗号化及び復号に必要な情報をライセンスするなどの方法も用いられている。

ところで、伝送路上のデータパケットのパケットヘッダに複製制御情報を格納して送る方式では、パケットが送信機器から受信機器に伝送される過程で、複製制御情報が他の機器により改竄される可能性がある。

例えば、図1に示すように、データ送信装置1側からデータパケットのパケットヘッダの複製制御情報をコピー禁止の意味を表す「1 1」で送信しても、伝送中に複製制御情報改竄攻撃があり、複製制御情報が1回コピー可を表す「1 0」に改竄されてしまうと、このパケットを受信したデータ受信装置2側では、このデータが本来コピー禁止であることを知ることができず、パケットヘッダの複製制御情報が1度の記録を許しているのでデータを記録してしまう。

このように、従来のデータ伝送方法では、コピー世代管理ができなくなってしまう恐れがある。

## 発明の開示

そこで、本発明の目的は、上述の如き従来の問題点に鑑み、コピー世代管理を確実に行うことができるデータ伝送システム、データ伝送方法、データ送信装置、データ送信方法、データ受信装置及びデータ受信方法を提供することにある。

本発明に係るデータ伝送システムは、データ受信装置との間で秘密に共有されている第1の情報と、データの複製制御情報から導かれる第2の情報と、上記データ受信装置との間で共有する時変情報である第3の情報に基づいて暗号鍵を生成し、上記暗号鍵を用いてデータを暗号化し、暗号化したデータに上記複製制御情報及び時変情報に基づく制御情報を付加した送信データを送信するデータ送信装置と、上記データ送信装置から送られてくる制御情報が付加され暗号化されたデータを受信し、上記データ送信装置との間で秘密に共有されている第1の情報と、上記受信データの制御情報から導かれる第2の情報と、上記データ送信装置との間で共有する時変情報である第3の情報に基づいて暗号鍵を生成し、上記暗号鍵を用いて上記受信データを復号するデータ受信装置とからなる。

また、本発明に係るデータ伝送方法では、データ送信装置とデータ受信装置の間で秘密に共有されている第1の情報と、送信データの複製制御情報から導かれる第2の情報と、データ受信装置との間で共有する時変情報である第3の情報によって生成された暗号鍵を用いてデータを暗号化して伝送する。

また、本発明に係るデータ伝送方法では、データ送信装置において、データ受信装置との間で秘密に共有されている第 1 の情報と、データの複製制御情報から導かれる第 2 の情報と、上記データ受信装置との間で共有する時変情報である第 3 の情報に基づいて暗号鍵を生成し、上記暗号鍵を用いてデータを暗号化し、暗号化したデータに上記複製制御情報及び時変情報に基づく制御情報を付加した送信データを送信し、データ受信装置において、上記データ送信装置から送られてくる制御情報が付加され暗号化されたデータを受信し、上記データ送信装置との間で秘密に共有されている第 1 の情報と、上記受信データの制御情報から導かれる第 2 の情報と、上記データ送信装置との間で共有する時変情報である第 3 の情報に基づいて暗号鍵を生成し、上記暗号鍵を用いて上記受信データを復号する。

また、本発明に係るデータ送信装置は、データ受信装置との間で秘密に共有されている第 1 の情報と、データの複製制御情報から導かれる第 2 の情報と、上記データ受信装置との間で共有する時変情報である第 3 の情報に基づいて暗号鍵を生成し、この暗号鍵を用いてデータを暗号化する暗号化処理手段と、この暗号化処理手段により暗号化したデータに上記複製制御情報及び時変情報に基づく制御情報を付加した送信データを送信する送信手段とを備える。

また、本発明に係るデータ送信方法では、データ受信装置との間で秘密に共有されている第 1 の情報と、データの複製制御情報から導かれる第 2 の情報と、上記データ受信装置との間で共有する時変情報である第 3 の情報に基づいて暗号鍵を生成し、この暗号鍵を用いてデータを暗号化し、暗号化したデータに上記複製制御情報及び時変情報に基づく制御情報を付加した送信データを送信する。

また、本発明に係るデータ受信装置は、データ送信装置から送られてくる複製制御情報及び時変情報に基づく制御情報が付加され暗号化されたデータを受信する受信手段と、この受信手段により受信された受信データについて、上記データ送信装置との間で秘密に共有されている第1の情報と、上記受信データの制御情報から導かれる第2の情報と、上記データ送信装置との間で共有する時変情報である第3の情報に基づいて暗号鍵を生成し、上記暗号鍵を用いて上記受信データを復号する復号処理手段とを備える。

さらに、本発明に係るデータ受信方法では、データ送信装置から送られてくる複製制御情報及び時変情報に基づく制御情報が付加され暗号化されたデータを受信し、この受信データについて、上記データ送信装置との間で秘密に共有されている第1の情報と、上記受信データの制御情報から導かれる第2の情報と、上記データ送信装置との間で共有する時変情報である第3の情報に基づいて暗号鍵を生成し、上記暗号鍵を用いて上記受信データを復号する。

#### 図面の簡単な説明

図1は、複製制御情報改竄攻撃による影響を説明するための図である。

図2は、本発明を適用したデータ伝送システムの構成を示すブロック図である。

図3は、IEEE1394シリアルバス上を伝送される伝送フレーム（アイソクロナス・パケット）の構成を示す図である。



図 4 は、上記データ伝送システムにおける認証・鍵共有プロトコルの実行手順を示すフローチャートである。

図 5 は、上記認証・鍵共有プロトコルにおけるデータ送信装置側の処理手順を示すフローチャートである。

図 6 は、上記認証・鍵共有プロトコルにおけるデータ受信装置側の処理手順を示すフローチャートである。

図 7 は、上記データ伝送システムにおけるデータ伝送処理の手順を示すフローチャートである。

図 8 は、上記データ伝送処理におけるデータ受信装置側の処理手順を示すフローチャートである。

図 9 は、上記データ伝送処理におけるデータ受信装置側の処理手順を示すフローチャートである。

#### 発明を実施するための最良の形態

以下、本発明を実施するための最良の形態について図面を参照しながら詳細に説明する。

本発明は、例えば図 2 に示すような構成のデータ伝送システムに適用される。

このデータ伝送システムは、データ送信装置 10 とデータ受信装置 20 を備え、データ送信装置 10 とデータ受信装置 20 が伝送路 30 を介して接続された構成となっている。

この実施の形態のデータ伝送システムにおいて、データ送信装置 10 は、例えば、通信衛星から送られてくる衛星デジタル多チャネ

ル放送番組を受信するセットトップボックスであって、内部バス 11 に接続された中央演算処理ユニット(CPU: Central Processing Unit) 12、メモリ 13、入力インターフェース 14、ユーザインターフェース 15、入出力インターフェース 16 等により構成されている。入力インターフェース 14 には衛星アンテナ 18 が接続されている。また、入出力インターフェース 16 は、デジタルインターフェースである I E E E(The International of Electrical and Electronics Engineers, Inc.) 1394 ハイ・パフォーマンス・シリアル・バス・インターフェース(以下、単に I E E E 1394 インターフェースという)であって、上記伝送路 30 に接続されている。伝送路 30 は、I E E E 1394 シリアルバスで構成される伝送路である。

このデータ送信装置 10 において、CPU 12 は、メモリ 13 に記憶されている制御プログラムにしたがって動作して、ユーザインターフェース 15 を介して入力される操作情報に応じて番組の選局動作等の各種制御動作を行うようになっている。

そして、このデータ送信装置 10 は、上記受信アンテナ 18 が接続された入力インターフェース 14 により衛星デジタル多チャンネル放送信号の所望のチャンネルを選局して所望のチャンネルの映像データや音楽データを受信し、受信した映像データや音楽データをコンテンツデータとして入出力インターフェース 16 から上記伝送路 30 に送信する。

また、データ受信装置 20 は、データ送信装置 10 により受信したコンテンツデータ、すなわち映像データや音楽データを磁気テープや光磁気ディスクなどの記録媒体に記録する記録装置であって、

内部バス 21 に接続された中央演算処理ユニット(CPU: Central Processing Unit) 22、メモリ 23、入出力インターフェース 24、ユーザインターフェース 25、メディアアクセス部 26 等により構成されている。入出力インターフェース 24 は、デジタルインターフェースである I E E E 1 3 9 4 インターフェースであって、伝送路 30 が接続されている。

I E E E 1 3 9 4 規格では、ネットワーク内で行われる伝送動作をサブアクションと呼び、次の 2 種類のサブアクションが規定されている。すなわち、2 つのサブアクションとして、「アシンクロナス(Asynchronous) データ転送」と呼ばれる通常のデータ伝送を行う非同期伝送モード及び、「アイソクロナス(Isochronous) データ転送」と呼ばれる伝送帯域を保証した同期伝送モードが定義されている。

このデータ伝送システムでは、伝送帯域を確保できる Isochronous データ転送を用いて音楽データをデータ送信装置 10 とデータ受信装置 20 との間で伝送する。

ここで、伝送路 30 である I E E E 1 3 9 4 シリアルバス上を Isochronous 転送で伝送されるパケット (アイソクロナス・パケット) の構成を図 3 に示す。

すなわち、アイソクロナス・パケットは、図 3 に示すように、ヘッダ、ヘッダ CRC、データフィールド及びデータ CRC で構成される。

ヘッダは、データ長(data\_length)、タグ(tag)、チャンネル(channel)、t コード(tcode)、複製制御情報、Odd/Even ビット及び同期コード sy を含んでいる。

データ長(data\_length)は、データフィールドの長さを示す。タグ(tag)は、アイソクロナス・パケットが伝送するデータのフォーマットを示す。チャンネル(channel)は、IEEE 1394シリアルバス上で伝送される複数のアイソクロナス・パケットから所定の所望のパケットの識別を行い、受信するために用いられる。tコード(tcode)は、トランザクション・コードであり、アイソクロナス転送であることを示す値が入る。Odd/Evenビットは、コンテンツキーをKcを計算する元となる情報の一つである時変情報を与える。複製制御情報は、コンテンツデータの複製の可否を示す。同期コードsyは、送信側と受信側で同期情報をやり取りするのに用いられ、映像データ及び音声データなどのデータフィールドに格納されたコンテンツデータの同期を取るのに使用される。

ヘッダCRCは、ヘッダに格納されたデータに対するCRC (Cyclic Redundancy Code) の格納される領域である。これに基づいてヘッダの伝送エラーのチェックが行われる。

データフィールドは、映像データや音声データ等のコンテンツデータが格納されるフィールドである。

データCRCは、データフィールドに格納されたデータに対するCRC (Cyclic Redundancy Code) の格納される領域である。これに基づいてデータの伝送エラーのチェックが行われる。

そして、データ受信装置20は、入出力インターフェース24を介してコンテンツデータを受信し、それが記録可能であれば、メディアアクセス部26により磁気テープや光磁気ディスクなどの記録媒体に記録する。

また、データ受信装置20は、記録禁止のコンテンツデータを受

信した場合には、メディアアクセス部 26 により記録媒体に記録することなく、単に、音楽データを音声出力端子 26 A から出力し、また映像データを映像出力端子 26 B から出力する。

このデータ受信装置 20 において、CPU 22 は、メモリ 23 に記憶されている制御プログラムにしたがって動作して、ユーザインターフェース 25 を介して入力される操作情報に応じて、記録媒体に対してメディアアクセス部 26 による記録する動作及び再生する動作等の各種制御動作を行うようになっている。

このデータ伝送システムにおいて、コンテンツデータは、次のようにして、暗号鍵（コンテンツキー Kc）により暗号化されてアイソクロナス・パケットのデータフィールドに格納され、そのアイソクロナス・パケットのヘッダに格納される時変情報（時変値 Nc）を与える Odd/Even ビットとコンテンツデータの複製の可否を示す複製制御情報とともに伝送される。

すなわち、データ伝送システムを構成するデータ送信装置 10 及びデータ受信装置 20 は、それぞれ固有又は共通の秘密情報を予め持っている。すなわち、公開鍵方式の場合には固有の秘密情報を持ち、共通鍵方式の場合は共通の秘密情報を持つ。例えば、各機器が製造される際に鍵管理機関から与えられる機器用の鍵を機器内にもっている。ここでは、機器用の鍵として共通の秘密情報を持っているものとする。また、各機器は、鍵管理機関から与えられる複製制御情報のそれぞれのステートに対応する n（例えば n = 64）ビットの定数を機器内に保存している。すなわち、各機器は、もともとコピー禁止を表す複製制御情報「11」（Copy-never）に対応する定数 Ca、一世代のみコピー可を表す複製制御情報「10」（Copy-on

e-generation)に対応する定数  $C_b$ 、“Copy-one-generation”だったコンテンツが一度記録されたコンテンツであることを表し、これ以上のコピー禁止を表す複製制御情報「01」(No-more-copies)に対応する定数  $C_c$ 、及び、コピー制限なしを表す複製制御情報「00」(Copy-freely)に対応する定数  $C_d$  をもっている。

データ送信装置10は、データを送信するに当たり、例えば  $m$  ビットの乱数を2つ生成し、一方を認証・鍵共有プロトコルの実行の際にデータ受信装置20に送られるエクスチェンジキー  $K_x$  とし、他方をデータ伝送の際に使用する時変値  $N_c$  の初期値とする。エクスチェンジキー  $K_x$  は、コンテンツキー  $K_c$  を計算する元となる情報の一つであって、認証・鍵共有プロトコルにより共有された鍵を用いてデータ送信装置10からデータ受信装置20に送られる。そして、データを送信する際に、そのデータに応じて複製制御情報をパケットヘッダに書き込む。次に、エクスチェンジキー  $K_x$  と時変値  $N_c$  (アイソクロナス・パケットのヘッダに格納される時変情報)と複製制御情報を用いて、コンテンツキー  $K_c$  を計算し、コンテンツキー  $K_c$  を用いてデータを暗号化して、アイソクロナス・パケットのデータフィールドに格納して、パケットヘッダと共に伝送路に送信する。

コンテンツキー  $K_c$  は、例えば複製制御情報が「10」であるとき、例えば次のように、

$$K_c = J [K_x, N_c, C_b]$$

にて計算する。

ここで、関数  $J$  は、出力から入力を求めることが困難な関数（一方向関数）である。関数  $J$  の具体例としては、例えば  $FIPS$  (Fed

eral Information Processing Standard) 180-1のSHA(Secure Hash Algorithm)-1を用いることができ、また、DES(Data Encryption Standard)等のブロック暗号を用いて構成することも可能である。

SHA-1を用いた場合、SHA-1に $K_x$ 、 $N_c$ 、 $C_b$ のビット連結( $K_x \parallel N_c \parallel C_b$ )を入力する。なお、必要に応じて関数 $J$ の出力(例えばSHA-1を用いた場合には160ビット)を、暗号アルゴリズムの鍵ビット数(例えばDESの場合には56ビット)に拡大、縮小してコンテンツキー $K_c$ とするようにしてもよい。拡大する場合には、例えば出力を複数回繰返し並べれば良く、縮小するには、上位あるいは下位の必要ビット数だけを使用する。

DESやSHA-1などの暗号技術については、Bruce Schneier 著「Applied Cryptography(Second Edition),Wiley」に詳しく解説されている。

さらに、データ送信装置10は、時変値 $N_c$ に応じて、データパケットのOdd/Evenビットの値をセットする。例えば時変値 $N_c$ の最下位ビットとOdd/Evenビットの値が一致するようにセットする。ここで、データ送信装置10は、例えば30秒以上2分以内など時間条件により、あるいは、伝送開始又は前回の更新から送信したデータのバケット数やバイト数等のデータ量の条件により、時変値 $N_c$ を更新する。時変値 $N_c$ の更新は、所定の時間間隔もしくは送信量をタイミングとしてインクリメントすることにより行う。そして、時変値 $N_c$ の更新に応じて新たにコンテンツキー $K_c$ を計算し、このコンテンツキー $K_c$ でコンテンツを暗号化してバケットに格納する。また、データパケットのOdd/Evenビ

ットの値を変化させる。

このデータ伝送システムでは、上記データ伝送に先立って、データ送信装置 10 とデータ受信装置 20 の間で互いの機器の認証と暗号鍵を共有するためのプロトコルを実行する。具体的には、図 4 のフローチャートに示すような認証・鍵共有プロトコルを実行してから、データ伝送を行う。なお、このデータ伝送システムにおけるデータ送信装置 10 側の処理手順を図 5 のフローチャートに示すとともに、データ受信装置 20 側の処理手順を図 6 のフローチャートに示す。

ここで、この認証・鍵共有プロトコルを示す図 4 では、データ送信装置 10 を Source Device A で表し、データ受信装置 20 を Sink Device B で表す。

そして、このデータ伝送システムにおいて、データ送信装置 10 の CPU 12 は、まず、データの伝送を開始するためのスタートコマンドを上記入出力インターフェース 16 から伝送路 30 を介してデータ受信装置 20 に送信する（ステップ S 10）。

データ受信装置 20 の CPU 22 は、入出力インターフェース 24 に接続された上記伝送路 30 を介して上記データ送信装置 10 から送られてくるスタートコマンド (START command) を受信したら（ステップ S 20）、 $m$ （例えば  $m = 64$ ）ビットの乱数  $R_B$  を生成し、この乱数  $R_B$  とデータ受信装置 20 の識別子  $ID_B$  のビット連結 ( $R_B \parallel ID_B$ ) を認証・鍵共有プロトコルの開始要求 (Request authentication) 共にデータ送信装置 10 に入出力インターフェース 24 を介して送信する（ステップ S 21）。

データ送信装置 10 の CPU 12 は、入出力インターフェース 1



6に接続された伝送路30を介してデータ受信装置20から送られてくる認証・鍵共有プロトコルの開始要求(Request authentication)とビット連結( $R_B \parallel ID_B$ )を受信したら(ステップS11)、 $m$ ビットの乱数 $R_A$ を生成し、

$$TokenAB = R_A \parallel MAC(K_{AB}, R_A \parallel R_B \parallel ID_B)$$

なる演算処理により、第1の認証情報 $TokenAB$ を求め、この第1の認証情報 $TokenAB$ をデータ受信装置20に入出力インターフェース16を介して送信する(ステップS12)。ここで、 $MAC$ は、ISO/IEC 9797に記載されている方式で作成されたメッセージ認証コード(Message Authentication Code)である。暗号関数としてはDESを使用する。また、 $K_{AB}$ は、データ送信装置10とデータ受信装置20の間で共有されている秘密情報である。すなわち、 $K_{AB}$ は、上述のように鍵管理機関から与えられた機器用の鍵である。

データ受信装置20のCPU22は、データ送信装置10から第1の認証情報 $TokenAB$ を受け取ったら(ステップS22)、 $K_{AB}$ 、 $R_A$ 、 $R_B$ 、 $ID_B$ を用いて独自に $MAC$ を計算し(ステップS23)、受信したものと一致することを確認する(ステップS24)。このステップS24において一致しなければ、データ受信装置20のCPU22は、データ送信装置10が不正な機器であると判断して、この認証・鍵共有プロトコルを終了する。

次に、データ受信装置20のCPU22は、 $m$ ビットの乱数 $S$ を生成し、

$$TokenBA = S \parallel MAC(K_{AB}, R_B \parallel R_A)$$

なる演算処理により、第2の認証情報 $TokenBA$ を求め、この

第2の認証情報TokenBAをデータ送信装置10に入出力インターフェース24を介して送る(ステップS25)。なお、上記乱数Sは、上記乱数R<sub>B</sub>と同じmビットでなくてもよい。ここで、データ受信装置20のCPU22は、MAC(K<sub>AB</sub>, S)の上位mビットを後述する一時キーとして使用する。

データ送信装置10のCPU12は、データ受信装置20から第2の認証情報TokenBAを受け取ったら(ステップS13)、K<sub>AB</sub>, R<sub>A</sub>, R<sub>B</sub>を用いて独自にMACを計算し(ステップS14)、受信したものと一致することを確認する(ステップS15)。このステップS15において、一致しなければ、データ送信装置10のCPU12は、データ受信装置20が不正な機器であると判断して、この認証・鍵共有プロトコルを終了する。そして、このステップS4において、一致したら、データ送信装置10のCPU12は、データ受信装置20を正当な機器であると認証し、MAC(K<sub>AB</sub>, S)の上位mビットを後述する一時キーとして使用する。

なお、MAC(K<sub>AB</sub>, S)の上位mビットを一時キーとして使用するが、そのビット数は、乱数Sと同じのビット数mと同じである必要はない。

次に、データ送信装置10のCPU12は、エクスチェンジキーK<sub>x</sub>を例えばDES暗号関数を用いて一時キーで暗号化し、暗号化したエクスチェンジキーK<sub>x</sub>をデータ受信装置20に入出力インターフェース16を介して送信する(ステップS16)。

そして、データ受信装置20は、データ送信装置10から送られてきた暗号化されたエクスチェンジキーK<sub>x</sub>をDES復号関数を用いて一時キーで復号して、エクスチェンジキーK<sub>x</sub>を得る(ステッ

プ S 2 6)。

このデータ伝送システムにおけるデータ受信装置 2 0 は、データ送信装置 1 0 との間で認証・鍵共有プロトコルを実行することにより得たエクステンジキー  $K_x$  及び時変値  $N_c$ 、データパケットの複製制御情報に対応した定数（この例では  $C_b$ ）から、コンテンツキー  $K_c$  をデータ送信装置 1 0 と同様に計算することができ、このコンテンツキー  $K_c$  を用いてデータを復号することができるようになる。

このデータ伝送システムでは、上記認証・鍵共有プロトコルを実行してから、図 7 のフローチャートに示すような手順に従ってデータ伝送を行う。このデータ伝送システムにおけるデータ受信装置 2 0 側の処理手順を図 8 のフローチャートに示すとともに、データ送信装置 1 0 側の処理手順を図 9 のフローチャートに示す。

すなわち、上記認証・鍵共有プロトコルによりエクステンジキー  $K_x$  を得たデータ受信装置 2 0 の CPU 2 2 は、次に、データ送信装置 1 0 に対し、現在の時変値  $N_c$  を送るように要求する（ステップ S 3 0）。

データ送信装置 1 0 の CPU 1 2 は、この  $N_c$  要求を受信すると（S 4 0）、この要求に応じて現在の時変値  $N_c$  を上記データ受信装置 2 0 に送信し（ステップ S 4 1）、この時変値  $N_c$  をデータ受信装置 2 0 が受信する（ステップ S 3 1）。

データ受信装置 2 0 は、データ送信装置 1 0 から送られてきた時変値  $N_c$  の最下位ビットとデータパケット中の Odd/Even ビットが等しいことを確認し、等しい場合に、時変値  $N_c$  とエクステンジキー  $K_x$ 、定数  $C_b$  からコンテンツキー  $K_c$  を計算する（ス

テップS 3 2)。時変値N cの最下位ビットとデータパケット中のOdd/Evenビットが等しくない場合には、データ受信装置20は、コンテンツキーK cが既に更新されたと判断し、送られた時変値N cをインクリメントした値を新たな時変値N cとして、コンテンツキーK cを計算する。

なお、上記N c要求に応じてデータ送信装置10から時変値N cをデータ受信装置20に送った後では、データ送信装置10及びデータ受信装置20は、共に、次の時変値N cの更新後の値が現在の値をインクリメントしたものであることが判っているので、予め次に使われるコンテンツキーK cを計算しておくことができる。

次に、データ送信装置10は、映像データや音声データなどのコンテンツデータを暗号鍵（コンテンツキーK c）で暗号化し、暗号化したコンテンツデータをアイソクロナス・パケットのデータフィールドに格納し、そのアイソクロナス・パケットのヘッダに格納される時変情報を与えるOdd/Evenビット及びコンテンツデータの複製制御情報とともに順次送信する（ステップS 4 2, S 4 3）。

すなわち、データ送信装置10では、例えば時変値N cに応じたOdd/Evenビットの設定状態を判定して（ステップS 4 1 A）、Odd/Evenビット=0であれば、Odd/Evenビット=0に対応するコンテンツキーK c（Oddキー）でコンテンツデータを暗号化した暗号化データを送信し（ステップS 4 2）、また、Odd/Evenビット=1であれば、Odd/Evenビット=1に対応するコンテンツキーK c（Evenキー）でコンテンツデータを暗号化した暗号化データを送信する処理を行う（ステ

ップS 4 3)。そして、送信終了か否かを判定し（ステップS 4 4）、その判定結果がNOすなわち送信終了でなければ、時変値N cの更新タイミングになったか否かを判定し（ステップS 4 5）、更新タイミングでなければ時変値N cを更新することなく上記Odd/Evenビットの設定状態の判定処理（ステップS 4 1 A）に戻り、更新タイミングになったら時変値N cをインクリメントすることにより更新するとともにOdd/Evenビットを更新し（ステップS 4 6）、上記Odd/Evenビットの設定状態の判定処理（ステップS 4 1 A）に戻ることににより、上記Odd/Evenビット=0に対応するコンテンツキーK c（Oddキー）でコンテンツデータを暗号化した暗号化データの送信処理（ステップS 4 2）と、Odd/Evenビット=1に対応するコンテンツキーK c（Evenキー）でコンテンツデータを暗号化した暗号化データの送信処理（ステップS 4 3）を繰り返し行う。

そして、上記送信終了か否かの判定処理（ステップS 4 4）のYESすなわち送信終了であれば、データ伝送モードの処理を終了する。

データ受信装置20は、このようにしてデータ送信装置10から送られてくる暗号化データを受信すると、計算したコンテンツキーK cを用いてデータを復号する（ステップS 3 3, S 3 4）。

すなわち、データ受信装置20では、暗号化データの受信受信復号処理（ステップS 3 3, S 3 4）を行う毎に、受信終了か否かを判定し（ステップS 3 5）、その判定結果がNOすなわち受信終了でなければ、時変値N cの更新タイミングになったか否かを判定し（ステップS 3 6）、更新タイミングでなければ時変値N cを更新

することなく上記コンテンツキー $K_c$ の計算処理（ステップS 3 2）に戻り、更新タイミングになったら時変値 $N_c$ をインクリメントすることにより更新して（ステップS 3 7）、上記コンテンツキー $K_c$ の計算処理（ステップS 3 2）に戻ることににより、上記 $O d d / E v e n$ ビット=0に対応する暗号化データの受信復号処理（ステップS 3 3）と、上記 $O d d / E v e n$ ビット=1に対応する暗号化データの受信送信処理（ステップS 3 4）を繰り返し行う。

データ受信装置20は、計算したコンテンツキー $K_c$ を用いてデータを復号することにより、このデータパケットに格納されていた複製制御情報に応じて、データの記録を可能にしたり禁止したりする制御を行うことができる。

なお、上述の実施の形態では、データ受信装置10が1台のデータ伝送システムについて説明したが、複数台のデータ受信装置がある場合にも、本発明は、そのまま適用することができる。

このような構成のデータ伝送システムにおいて、例えば、データ送信装置10側からデータパケットのパケットヘッダの複製制御情報をコピー禁止の意味表す「11」で送信した場合に、伝送中に複製制御情報改竄攻撃があり、複製制御情報が1回コピー可を表す「10」に改竄されてしまうと、このパケットを受信したデータ受信装置20側では、このデータの複製制御情報「10」に対応した定数 $C_b$ を用いてコンテンツキー $K_c$ を計算し、このコンテンツキー $K_c$ を用いてコンテンツデータを復号することになる。

データ送信装置10側におけるコンテンツデータの暗号化は、複製制御情報「11」に対応した定数 $C_a$ を用いて計算したコンテンツキー $K_c$ により行われているので、データ受信装置20側におい

て復号の結果として得られるデータは無意味なデータとなる。すなわち、データ受信装置 20 で現れるデータは、元のコンテンツデータではないので記録しても意味がなく、コピーの世代管理が崩れることはない。

また、このデータ伝送システムでは、コンテンツキー  $K_c$  に時変値  $N_c$  を作用させているので、この時変値  $N_c$  を頻繁に変えることにより、同一の暗号鍵を用いて暗号化されるデータの量を制限することができ、暗号解析のおそれを少なくすることができる。

さらに、時変値  $N_c$  の更新をインクリメントにより行い、現在使われている時変値に対応した値をデータパケットに格納して伝送することにより、データ受信装置 20 側で時変値  $N_c$  の更新を簡単に知ることができ、また、正しいコンテンツキー  $K_c$  をデータ送信装置 10 及びデータ受信装置 20 が共に予め計算しておくことができる。これにより、時変値  $N_c$  の更新がある毎に、データ受信装置 20 がデータ送信装置 10 に対して時変値  $N_c$  を問い合わせる必要もなく、システム全体としての通信量の抑制、制御ソフトウェアの簡略化を図ることができる。

また、コンテンツキー  $K_c$  を計算する際に、出力から入力を求めることが困難な一方向性関数を用いているので、仮に上記コンテンツキー  $K_c$  が露見したとしても、エクスチェンジキー  $K_x$  や複製制御情報に対応する定数が不正に求められてしまうことがない。したがって、あるコンテンツキー  $K_c$  が露見したとしても、別のコンテンツキー  $K_c$  を用いて暗号化されたコンテンツデータが解読されてしまうことはない。

以上のように本発明の実施の形態においては、データ送信装置か

らデータ受信装置にデータを一方伝送するに当たり、データ受信装置との間で秘密に共有されている第1の情報と、送信データの複製制御情報から導かれる第2の情報と、上記データ受信装置との間で共有する時変情報である第3の情報によって暗号鍵を生成し、この暗号鍵を用いてデータを暗号化し、暗号化したデータに上記複製制御情報及び時変情報を付加した送信データをデータ送信装置から送信することにより、データ受信装置側では、上記データ送信装置から送られてくる複製制御情報及び時変情報が付加され暗号化されたデータを受信し、受信された受信データについて、上記データ送信装置との間で秘密に共有されている第1の情報と、上記受信データの複製制御情報から導かれる第2の情報と、上記データ送信装置との間で共有する時変情報である第3の情報によって暗号鍵を生成し、この暗号鍵を用いて上記受信データを復号することができる。

このように送信データの暗号鍵に上記送信データの複製制御情報から導かれる第2の情報を暗号鍵に作用させておくことにより、伝送中に複製制御情報改竄攻撃によって複製制御情報が改竄されてしまった場合には、データ再生装置側で受信したデータの複製制御情報に応じた第2の情報に基づいて計算される暗号鍵はデータ送信装置側で使用した暗号鍵とは異なるものとなるので、受信データを正常に復号することができず、コピーの世代管理が崩れることはない。

また、暗号鍵に時変情報を作用させているので、この時変情報を頻繁に変えることにより、同一の暗号鍵を用いて暗号化されるデータの量を制限することができ、暗号解析のおそれを少なくすることができる。

さらに、時変情報の更新をインクリメントにより行い、現在使わ



れている時変情報に対応した値をデータパケットに格納して伝送することにより、データ受信装置側で時変情報の更新を簡単に知ることができ、また、正しい暗号鍵をデータ送信装置及びデータ受信装置が共に予め計算しておくことができる。これにより、時変情報の更新がある毎に、データ受信装置がデータ送信装置 10 に対して時変値  $N_c$  を問い合わせる必要もなく、システム全体としての通信量の抑制、制御ソフトウェアの簡略化を図ることができる。

また、上記暗号鍵を計算する際に、出力から入力を求めることが困難な一方向性関数を用いることにより、仮に上記暗号鍵が露見したとしても、データ受信装置との間で秘密に共有されている第 1 の情報や複製制御情報に対応する第 2 の情報が不正に求められてしまうことがない。したがって、ある暗号鍵が露見したとしても、別の暗号鍵を用いて暗号化されたデータが解読されてしまうことはない。

### 請求の範囲

1. データ受信装置との間で秘密に共有されている第1の情報と、データの複製制御情報から導かれる第2の情報と、上記データ受信装置との間で共有する時変情報である第3の情報に基づいて暗号鍵を生成し、上記暗号鍵を用いてデータを暗号化し、暗号化したデータに上記複製制御情報及び時変情報に基づく制御情報を付加した送信データを送信するデータ送信装置と、

上記データ送信装置から送られてくる制御情報が付加され暗号化されたデータを受信し、上記データ送信装置との間で秘密に共有されている第1の情報と、上記受信データの制御情報から導かれる第2の情報と、上記データ送信装置との間で共有する時変情報である第3の情報に基づいて暗号鍵を生成し、上記暗号鍵を用いて上記受信データを復号するデータ受信装置とからなるデータ伝送システム。

2. 上記データ送信装置及びデータ受信装置は、それぞれ上記第3の情報として予め定められた時間条件により変動する時変情報を用いて、上記暗号鍵を生成する請求の範囲第1項記載のデータ伝送システム。

3. 上記データ送信装置及びデータ受信装置は、それぞれ上記第3の情報として予め定められたデータ量の条件により変動する時変情報を用いて、上記暗号鍵を生成する請求の範囲第1項記載のデータ伝送システム。

4. 上記データ送信装置及びデータ受信装置は、それぞれ上記第3の情報として変動前の値を用いて変動後の値を求めることが可能

な時変情報を用いて、上記暗号鍵を生成する請求の範囲第1項記載のデータ伝送システム。

5. 上記データ受信装置は、上記受信データに付加された制御情報に基づいて上記時変情報である第3の情報の変化を検出し、上記第3の情報を更新する請求の範囲第4項記載のデータ伝送システム。

6. 上記データ受信装置は、上記受信データに付加された制御情報に基づいて上記時変情報である第3の情報の変化を検出し、更新前の上記第3の情報に対してインクリメント処理を施した値に基づいて更新された第3の情報を算出する請求の範囲第5項記載のデータ伝送システム。

7. 上記データ送信装置及びデータ受信装置は、それぞれ一方向関数を用いて、上記第1の情報と第2の情報と第3の情報から上記暗号鍵を生成する請求の範囲第1項記載のデータ伝送システム。

8. 暗号化されたデータを復号する装置で復号処理される伝送信号であって、

データの複製の許可状態を示す複製許可情報と、所定時間毎に更新される時変情報とを具備するヘッダと、

上記複製許可情報と上記時変情報とに基づく暗号鍵を用いて暗号化されたデータとを具備する伝送信号。

9. データ送信装置とデータ受信装置の間で秘密に共有されている第1の情報と、送信データの複製制御情報から導かれる第2の情報と、データ受信装置との間で共有する時変情報である第3の情報によって生成された暗号鍵を用いてデータを暗号化して伝送するデータ伝送方法。

10. 上記第3の情報として予め定められた時間条件により変動

する時変情報を用いて、上記暗号鍵を生成する請求の範囲第 9 項記載のデータ伝送方法。

1 1. 上記第 3 の情報として予め定められたデータ量の条件により変動する時変情報を用いて、上記暗号鍵を生成する請求の範囲第 9 項記載のデータ伝送方法。

1 2. 上記第 3 の情報として変動前の値を用いて変動後の値を求めることが可能な時変情報を用いて、上記暗号鍵を生成する請求の範囲第 9 項請求項記載のデータ伝送方法。

1 3. 一方向関数を用いて、上記第 1 の情報と第 2 の情報と第 3 の情報から上記暗号鍵を生成する請求の範囲第 9 項記載のデータ伝送方法。

1 4. データ送信装置において、データ受信装置との間で秘密に共有されている第 1 の情報と、データの複製制御情報から導かれる第 2 の情報と、上記データ受信装置との間で共有する時変情報である第 3 の情報に基づいて暗号鍵を生成し、上記暗号鍵を用いてデータを暗号化し、暗号化したデータに上記複製制御情報及び時変情報に基づく制御情報を付加した送信データを送信し、

データ受信装置において、上記データ送信装置から送られてくる制御情報が付加され暗号化されたデータを受信し、上記データ送信装置との間で秘密に共有されている第 1 の情報と、上記受信データの制御情報から導かれる第 2 の情報と、上記データ送信装置との間で共有する時変情報である第 3 の情報に基づいて暗号鍵を生成し、上記暗号鍵を用いて上記受信データを復号するデータ伝送方法。

1 5. 上記データ送信装置及びデータ受信装置において、それぞれ上記第 3 の情報として予め定められた時間条件により変動する時

変情報を用いて、上記暗号鍵を生成する請求の範囲第 1 4 項記載のデータ伝送方法。

1 6. 上記データ送信装置及びデータ受信装置において、それぞれ上記第 3 の情報として予め定められたデータ量の条件により変動する時変情報を用いて、上記暗号鍵を生成する請求の範囲第 1 4 項記載のデータ伝送方法。

1 7. 上記データ送信装置及びデータ受信装置において、それぞれ上記第 3 の情報として変動前の値を用いて変動後の値を求めることが可能な時変情報を用いて、上記暗号鍵を生成する請求の範囲第 1 4 項記載のデータ伝送方法。

1 8. 上記データ受信装置において、上記受信データに付加された制御情報に基づいて上記時変情報である第 3 の情報の変化を検出し、上記第 3 の情報を更新する請求の範囲第 1 4 項記載のデータ伝送方法。

1 9. 上記データ受信装置において、上記受信データに付加された制御情報に基づいて上記時変情報である第 3 の情報の変化を検出し、更新前の上記第 3 の情報に対してインクリメント処理を施した値に基づいて更新された第 3 の情報を算出する請求の範囲第 1 8 項記載のデータ伝送方法。

2 0. 上記データ送信装置及びデータ受信装置において、それぞれ一方向関数を用いて、上記第 1 の情報と第 2 の情報と第 3 の情報から上記暗号鍵を生成する請求の範囲第 1 4 項記載のデータ伝送方法。

2 1. データ受信装置との間で秘密に共有されている第 1 の情報と、データの複製制御情報から導かれる第 2 の情報と、上記データ

受信装置との間で共有する時変情報である第3の情報に基づいて暗号鍵を生成し、この暗号鍵を用いてデータを暗号化する暗号化処理手段と、

この暗号化処理手段により暗号化したデータに上記複製制御情報及び時変情報に基づく制御情報を付加した送信データを送信する送信手段と

を備えるデータ送信装置。

22. 上記暗号化処理手段は、上記第3の情報として予め定められた時間条件により変動する時変情報を用いて生成した暗号鍵により、データを暗号化する請求の範囲第21項記載のデータ送信装置。

23. 上記暗号化処理手段は、上記第3の情報として予め定められたデータ量の条件により変動する時変情報を用いて生成した暗号鍵により、データを暗号化する請求の範囲第21項記載のデータ送信装置。

24. 上記暗号化処理手段は、上記第3の情報として変動前の値を用いて変動後の値を求めることが可能な時変情報を用いて生成した暗号鍵により、データを暗号化する請求の範囲第21項記載のデータ送信装置。

25. 上記暗号化処理手段は、上記第1の情報と第2の情報と第3の情報から一方向関数を用いて生成した暗号鍵により、データを暗号化する請求の範囲第21項記載のデータ送信装置。

26. データ受信装置との間で秘密に共有されている第1の情報と、データの複製制御情報から導かれる第2の情報と、上記データ受信装置との間で共有する時変情報である第3の情報に基づいて暗号鍵を生成し、

この暗号鍵を用いてデータを暗号化し、

暗号化したデータに上記複製制御情報及び時変情報に基づく制御情報を付加した送信データを送信するデータ送信方法。

27. 上記第3の情報として予め定められた時間条件により変動する時変情報を用いて生成した暗号鍵により、データを暗号化する請求の範囲第26項記載のデータ送信方法。

28. 上記第3の情報として予め定められたデータ量の条件により変動する時変情報を用いて生成した暗号鍵により、データを暗号化する請求の範囲第26項記載のデータ送信方法。

29. 上記第3の情報として変動前の値を用いて変動後の値を求めることが可能な時変情報を用いて生成した暗号鍵により、データを暗号化する請求の範囲第26項記載のデータ送信方法。

30. 上記第1の情報と第2の情報と第3の情報から一方向関数を用いて生成した暗号鍵により、データを暗号化する請求の範囲第26項記載のデータ送信方法。

31. データ送信装置から送られてくる複製制御情報及び時変情報に基づく制御情報が付加され暗号化されたデータを受信する受信手段と、

この受信手段により受信された受信データについて、上記データ送信装置との間で秘密に共有されている第1の情報と、上記受信データの制御情報から導かれる第2の情報と、上記データ送信装置との間で共有する時変情報である第3の情報に基づいて暗号鍵を生成し、上記暗号鍵を用いて上記受信データを復号する復号処理手段とを備えるデータ受信装置。

32. 上記復号処理手段は、上記第3の情報として予め定められ

た時間条件により変動する時変情報を用いて生成した暗号鍵により、上記受信データを復号する請求の範囲第 3 1 項記載のデータ受信装置。

3 3. 上記復号処理手段は、上記第 3 の情報として予め定められたデータ量の条件により変動する時変情報を用いて生成した暗号鍵により、上記受信データを復号する請求の範囲第 3 1 項記載のデータ受信装置。

3 4. 上記復号処理手段は、上記第 3 の情報として変動前の値を用いて変動後の値を求めることが可能な時変情報を用いて生成した暗号鍵により、上記受信データを復号する請求の範囲第 3 1 項記載のデータ受信装置。

3 5. 上記復号処理手段は、上記受信データに付加された制御情報に基づいて上記時変情報である第 3 の情報の変化を検出し、上記第 3 の情報を更新する請求の範囲第 3 1 項記載のデータ受信装置。

3 6. 上記復号処理手段は、上記受信データに付加された制御情報に基づいて上記時変情報である第 3 の情報の変化を検出し、更新前の上記第 3 の情報に対してインクリメント処理を施した値に基づいて更新された第 3 の情報を算出する請求の範囲第 3 5 項記載のデータ受信装置。

3 7. 上記暗号化処理手段は、上記第 1 の情報と第 2 の情報と第 3 の情報から一方向関数を用いて生成した暗号鍵により、上記受信データを復号することを特徴とする請求の範囲第 3 1 項記載のデータ受信装置。

3 8. データ送信装置から送られてくる複製制御情報及び時変情報に基づく制御情報が付加され暗号化されたデータを受信し、



この受信データについて、上記データ送信装置との間で秘密に共有されている第1の情報と、上記受信データの制御情報から導かれる第2の情報と、上記データ送信装置との間で共有する時変情報である第3の情報に基づいて暗号鍵を生成し、上記暗号鍵を用いて上記受信データを復号するデータ受信方法。

39. 上記第3の情報として予め定められた時間条件により変動する時変情報を用いて生成した暗号鍵により、上記受信データを復号する請求の範囲第38項記載のデータ受信方法。

40. 上記第3の情報として予め定められたデータ量の条件により変動する時変情報を用いて生成した暗号鍵により、上記受信データを復号する請求の範囲第38項記載のデータ受信方法。

41. 上記第3の情報として変動前の値を用いて変動後の値を求めることが可能な時変情報を用いて生成した暗号鍵により、上記受信データを復号する請求の範囲第38項記載のデータ受信装置。

42. 上記受信データに付加された制御情報に基づいて上記時変情報である第3の情報の変化を検出し、上記第3の情報を更新する請求の範囲第38項記載のデータ受信方法。

43. 上記受信データに付加された制御情報に基づいて上記時変情報である第3の情報の変化を検出し、更新前の上記第3の情報に対してインクリメント処理を施した値に基づいて更新された第3の情報を算出する請求の範囲第42項記載のデータ受信方法。

44. 上記第1の情報と第2の情報と第3の情報から一方向関数を用いて生成した暗号鍵により、上記受信データを復号することを特徴とする請求の範囲第38項記載のデータ受信方法。

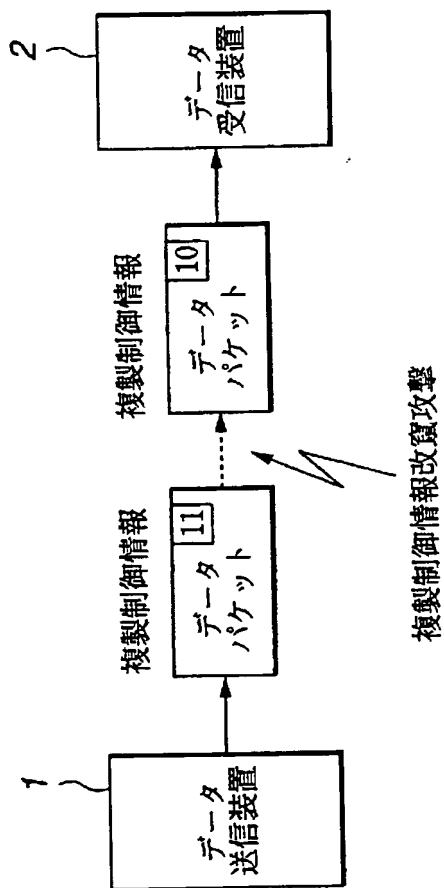


FIG.1

2/9

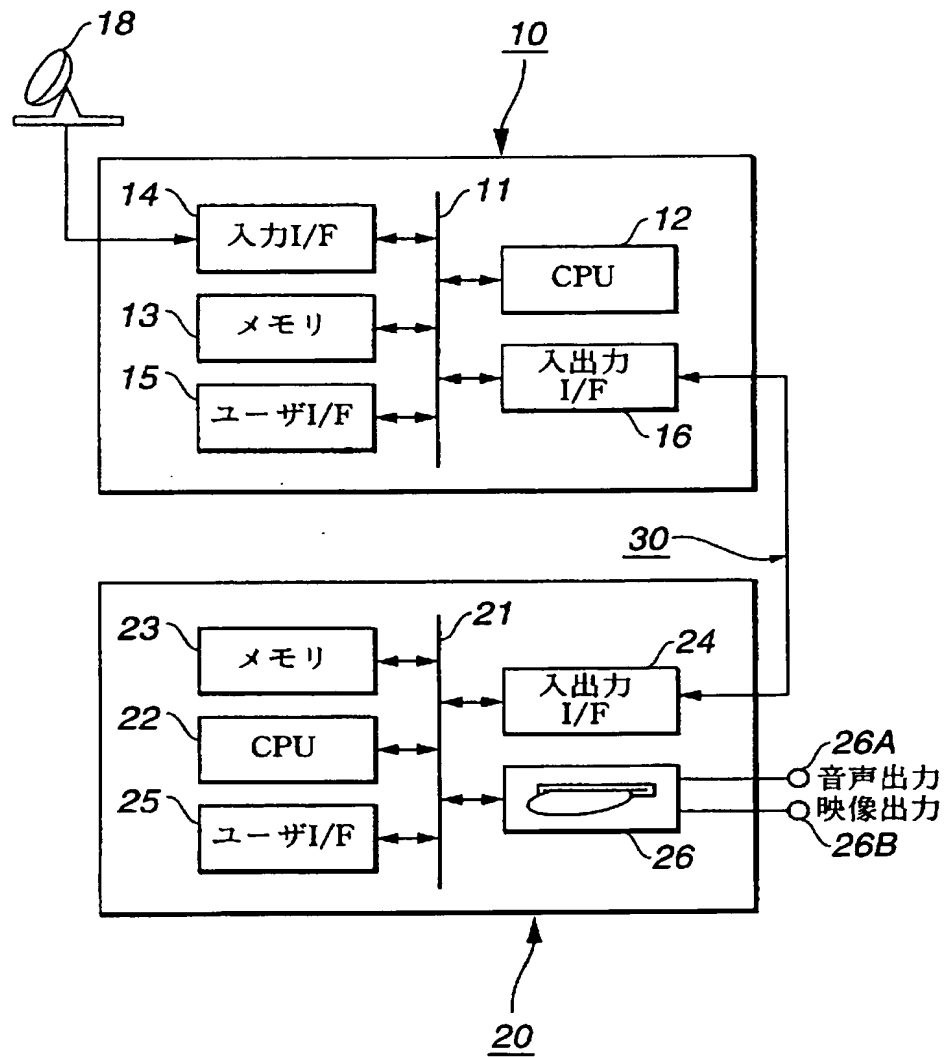


FIG.2

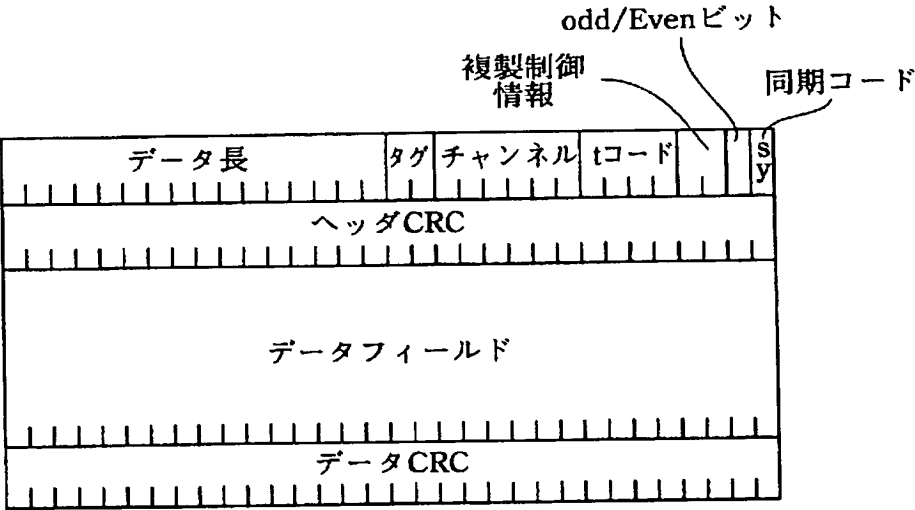


FIG.3

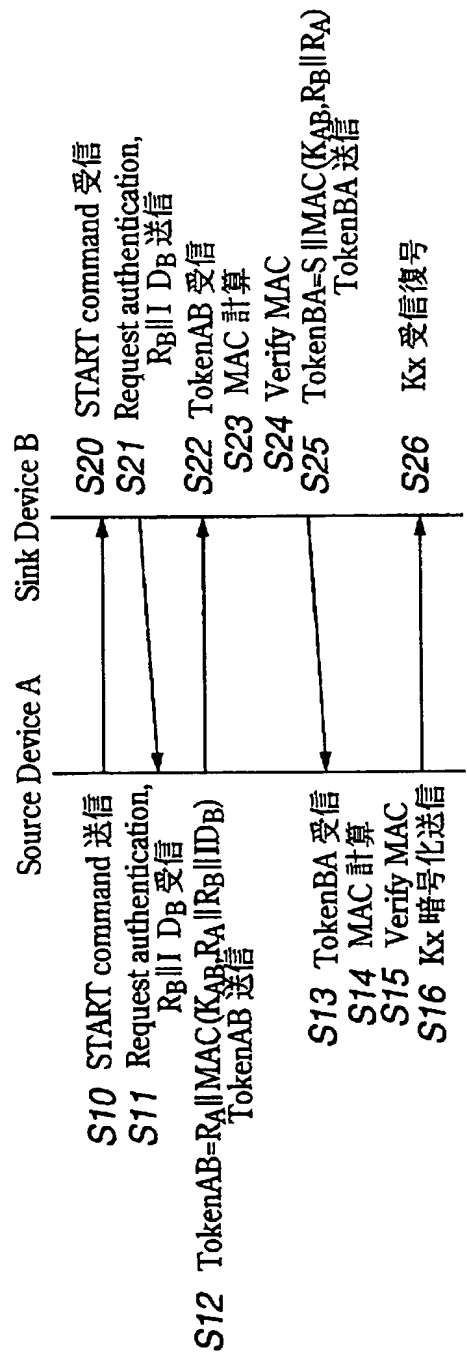


FIG.4

5/9

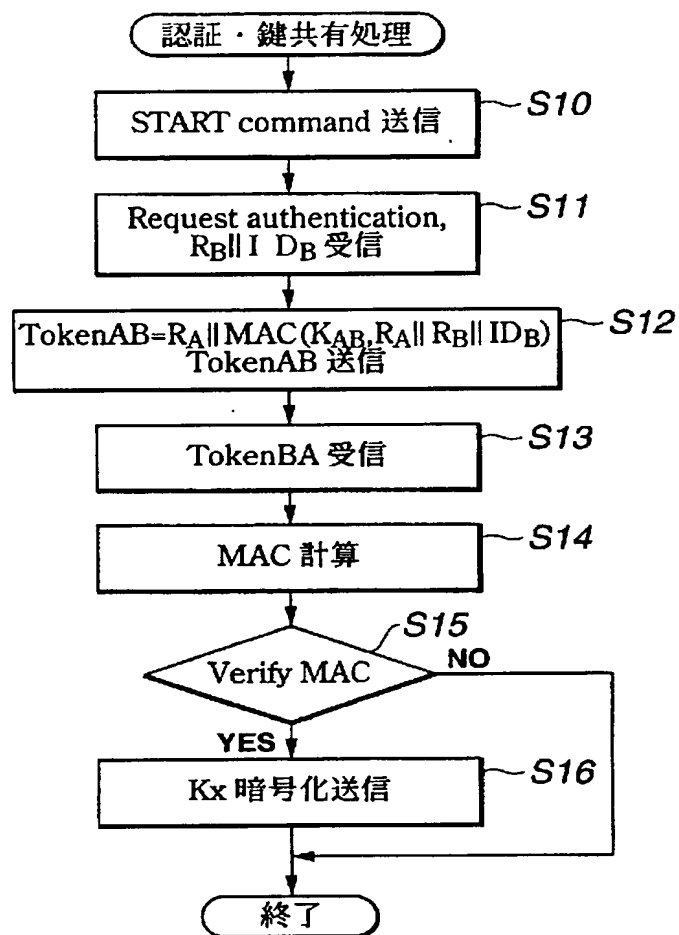


FIG.5

6/9

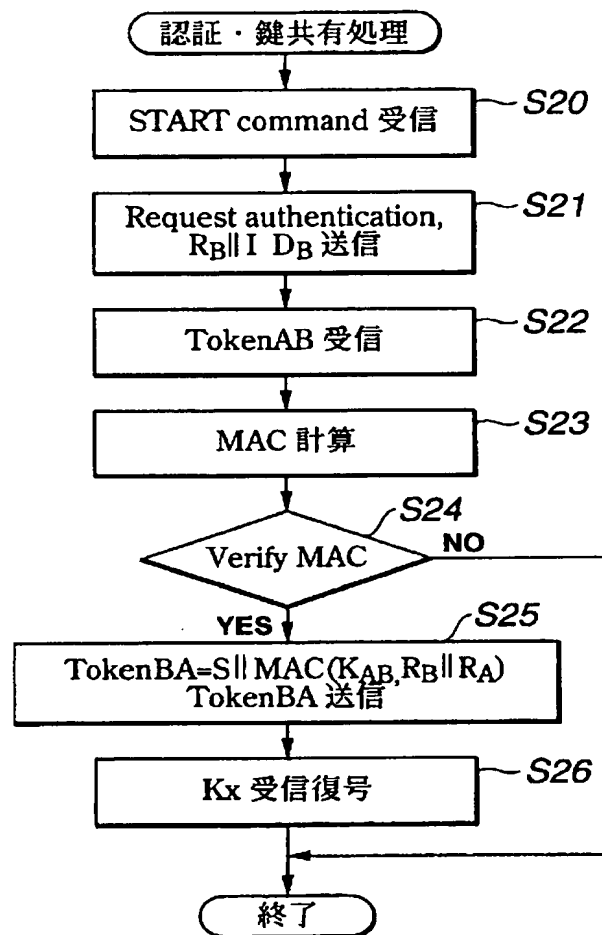


FIG.6

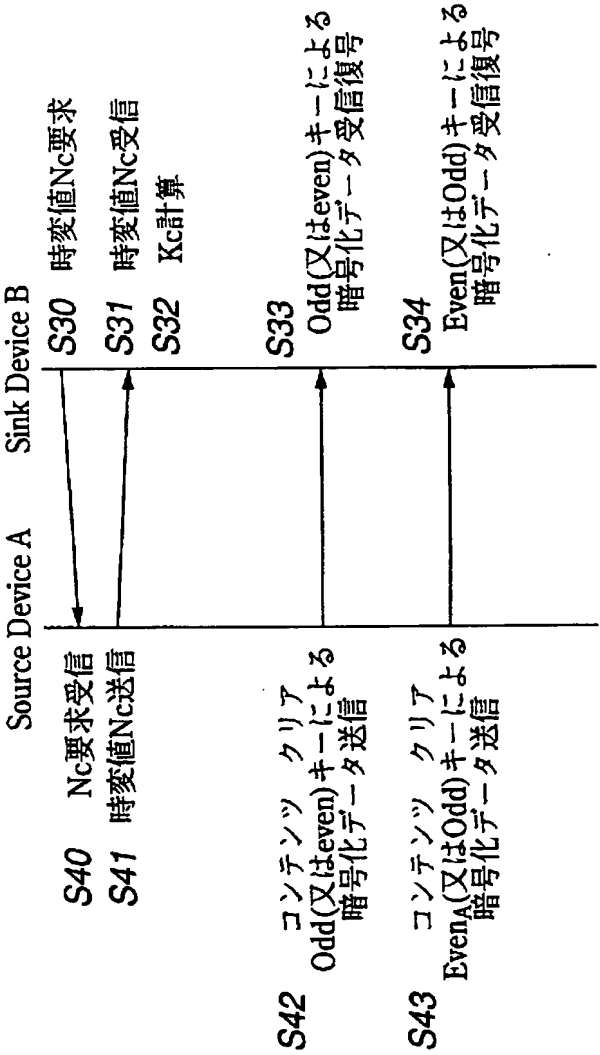


FIG.7



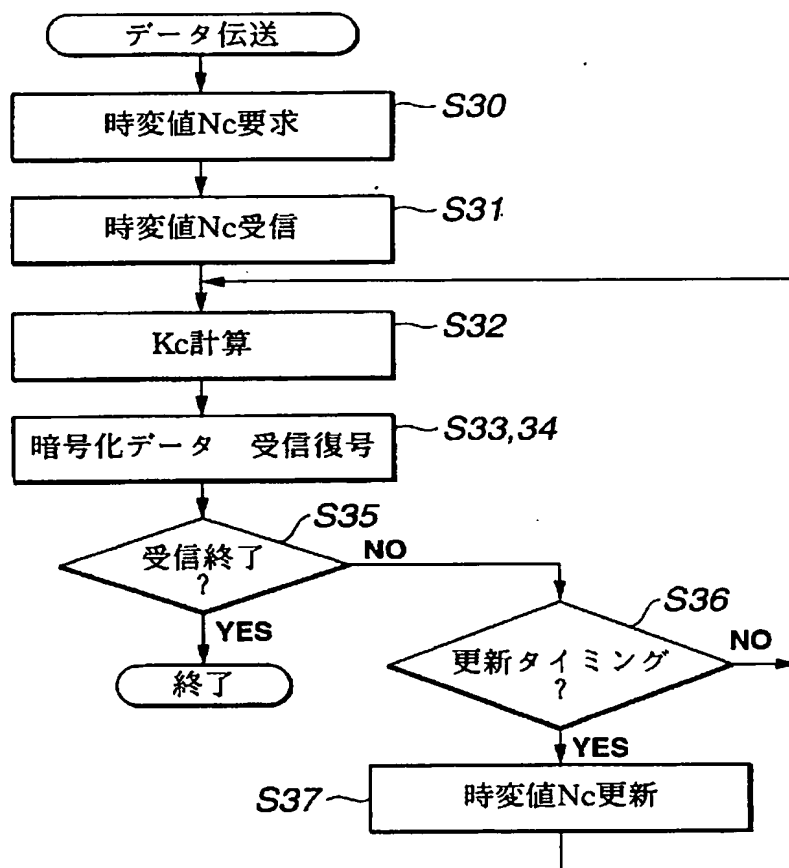


FIG.8

9/9

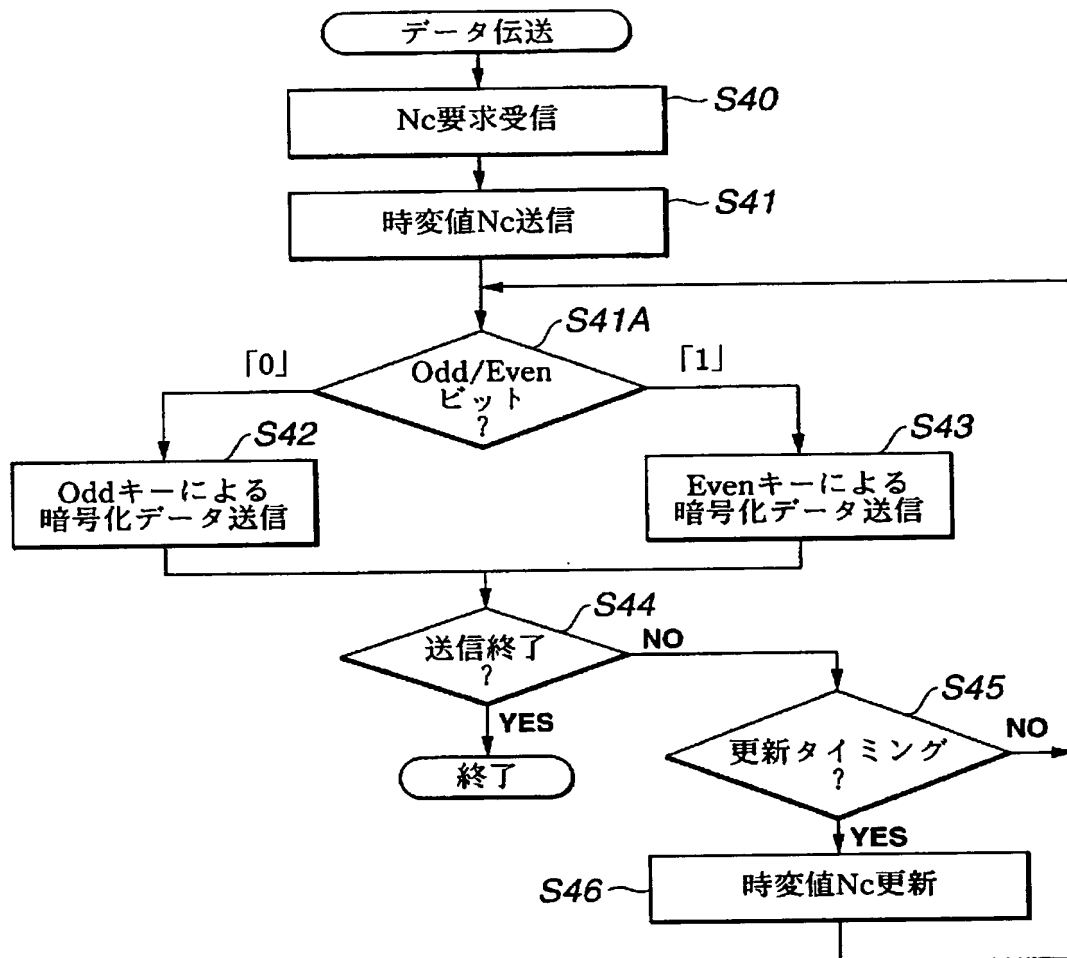


FIG.9

## INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP00/02354

## A. CLASSIFICATION OF SUBJECT MATTER

Int.Cl.<sup>7</sup> H04L9/08, H04L9/32, H04L12/40, H04N7/167

According to International Patent Classification (IPC) or to both national classification and IPC

## B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Int.Cl.<sup>7</sup> H04L9/08, H04L9/32, H04L12/40, H04N7/167

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho 1926-1996 Toroku Jitsuyo Shinan Koho 1994-2000

Kokai Jitsuyo Shinan Koho 1971-2000 Jitsuyo Shinan Toroku Koho 1996-2000

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

## C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	Ryuji Ishiguro "Angou Gijutsu wo Tsukatta IEEE1394 jo no Computer Protection", Proceedings of Sony Research Forum 1997, Vol.7th (01.02.98) p.203-208	1-44
Y	Hitachi, Ltd. et al., "5C Digital Transmission Content Protection White Paper", Revision 1.0 http://www.dtcp.com/wp_spec.pdf (14.07.98)	1-44
Y	JP, 4-277951, A (NEC Corporation), 02 October, 1992 (02.10.92), page 1, Column 1, lines 1 to 30; Figs. 1 to 7 & EP, 502441, A & CA, 2062170, A & US, 5251258, A & DE, 69227936, A	1,8,9,14, 21,26,31,38
Y	JP, 1-165241, A (Mitsubishi Electric Corporation), 29 June, 1989 (29.06.89), page 2, lower right column, lines 1 to 13; Figs. 1 to 2 (Family: none)	1,9,14,21, 26,31,38
Y	JP, 10-4403, A (NTT Data Tsushin K.K.), 06 January, 1998 (06.01.98),	4,12,17,24, 29,34,41

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:	"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A" document defining the general state of the art which is not considered to be of particular relevance	"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E" earlier document but published on or after the international filing date	"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&" document member of the same patent family
"O" document referring to an oral disclosure, use, exhibition or other means	
"P" document published prior to the international filing date but later than the priority date claimed	

Date of the actual completion of the international search  
04 July, 2000 (04.07.00)Date of mailing of the international search report  
18 July, 2000 (18.07.00)Name and mailing address of the ISA/  
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

## INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP00/02354

## C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
	page 5, Column 7, line 10 to page 6, Column 9, line 2; Figs. 1 to 4 (Family: none)	
A	Teruyoshi Komuro "Av wo Multi Media ka Suru IEEE1394 no Genjo to Tenbo" Denshi Gijutsu March, Vol.41, No.3 (01.03.99) pp.2-7	1-44
A	JP, 10-303945, A (Sony Corporation), 13 November, 1998 (13.11.98), Full text; Figs. 1 to 6 & KR, 98081633, A	1-44

## 国際調査報告

国際出願番号 PCT/JPO0/02354

## A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int. Cl<sup>7</sup> H04L9/08, H04L9/32, H04L12/40, H04N7/167

## B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))

Int. Cl<sup>7</sup> H04L9/08, H04L9/32, H04L12/40, H04N7/167

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報 1926-1996年  
 日本国公開実用新案公報 1971-2000年  
 日本国登録実用新案公報 1994-2000年  
 日本国実用新案登録公報 1996-2000年

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

## C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
Y	石黒隆二: “暗号技術を使ったIEEE1394上のコンピュータ プロテクション” Proceedings of Sony Research Forum 1997 (ソニーリサーチフォー ラム1997論文集), Vol. 7th (01.02.98) p. 203-208	1-44
Y	Hitachi, Ltd. 他: “5C Digital Transmission Content Protection White Paper”, Revision1.0 <a href="http://www.dtcp.com/wp_spec.pdf">http://www.dtcp.com/wp_spec.pdf</a> (14.07.98)	1-44

☒ C欄の続きにも文献が列举されている。☐ パテントファミリーに関する別紙を参照。

## \* 引用文献のカテゴリー

- 「A」 特に関連のある文献ではなく、一般的技術水準を示すもの  
 「E」 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの  
 「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)  
 「O」 口頭による開示、使用、展示等に言及する文献  
 「P」 国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

- 「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの  
 「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの  
 「Y」 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの  
 「&」 同一パテントファミリー文献

国際調査を完了した日

04.07.00

国際調査報告の発送日

18.07.00

国際調査機関の名称及びあて先

日本国特許庁 (ISA/JP)  
 郵便番号100-8915  
 東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)

青木 重徳

5W

4229

電話番号 03-3581-1101 内線 3574

C (続き) . 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
Y	JP, 4-277951, A (日本電気株式会社) 2. 10月. 1992 (02. 10. 92) 第1頁第1欄第1-30行, 図1-7 & EP, 502441, A & CA, 2062170, A & US, 5251258, A & DE, 69227936, A	1, 8, 9, 14, 21, 26, 31, 38
Y	JP, 1-165241, A (三菱電機株式会社) 29. 6月. 1989 (29. 06. 89) 第2頁右下欄第1-13行, 第1-2図 (ファミリーなし)	1, 9, 14, 21, 26, 31, 38
Y	JP, 10-4403, A (エヌ・ティ・ティ・データ通信株式 会社) 6. 1月. 1998 (06. 01. 98) 第5頁第7欄第10行-第6頁第9欄第2行, 図1-4 (ファミリーなし)	4, 12, 17, 24, 29, 34, 41
A	小室輝芳; "AVをマルチメディア化するIEEE1394の現状 と展望" 電子技術 3月号, Vol. 41, No. 3 (01. 03. 99) p. 2-7	1-44
A	JP, 10-303945, A (ソニー株式会社) 13. 11月. 1998 (13. 11. 98) 全文, 図1-6 & KR, 98081633, A	1-44